Kryptographie - Projekt / Praktikum

Thema: Die Kryptographie bezeichnet Methoden, mit denen vertrauliche Kommunikation über Netzwerke möglich ist. Dazu gehören Ver- und Entschlüsselungsverfahren, Verfahren zum Schlüsselaustausch, Hashfunktionen zur Gewährleistung von Datenintegrität, komplexere Protokolle wie für die Gesundheitskarte, Identifikationsverfahren wie Zero-Knowledge, Digitale Signaturen, und mehr.

In dem angebotenen Projekt werden einige Fragestellungen untersucht, die Gegenstand aktueller Kryptographie-Forschung sind. Insbesondere geht es um Sicherheitsanalysen von Hashfunktionen und Stromchiffren. In beiden Gebieten existieren bereits Verfahren, wobei die meisten davon nicht mehr als kryptographisch sicher betrachtet werden. Das Entwickeln neuer Verfahren und die Sicherheitsanalyse dieser wirft nun neue Fragestellungen auf.

Ablauf: Das "Algorithmen Projekt: Kryptographie" findet im **Sommer-Semester 2009** statt (Start in der ersten Semesterwoche). Die Veranstaltung kann als **Projekt oder Praktikum** besucht werden. Zu Beginn der Veranstaltung werden 1 bis 3 Kryptographie-Themen ausgewählt, hierbei können von den Teilnehmern Vorschläge gemacht werden.

Außerdem werden Kryptographie-Themen für eine **Bachelor oder Masterarbeit** angeboten (diese können bereits in der vorlesungsfreien Zeit starten).

Voraussetzungen: Die Veranstaltung richtet sich an Studenten der Informatik oder Mathematik. Es ist nicht notwenig bereits eine Kryptographie-Vorlesung besucht zu haben. Hilfreich sind grundlegende Kenntnisse in diskreter Mathematik und Wahrscheinlichkeitsrechnung sowie in theoretischer Informatik.

Anspruch: In der Veranstaltung wird es zunächst darum gehen den aktuellen Stand der Kryptographie-Forschung (in ausgewählten Bereichen) aufzuarbeiten. Dieser Teil der Veranstaltung hat den Charakter einer Literaturarbeit. Danach soll das erarbeitete Wissen praktisch umgesetzt werden, durch eigene Implementierungen und Experimente.
Teilnehmer der Veranstaltung bekommen so einen Eindruck wie wissenschftliches Arbeiten in der theoretischen Informatik abläuft. Das Ziel der jeweiligen Themenstellung wird immer sein, einen Beitrag zur aktuellen Forschung zu leisten, was aber nicht notwendig erreicht werden muss.

Betreuung: durch Dr. Tobias Eibach und Prof. Uwe Schöning. Bei Interesse bitte mit T. Eibach Kontakt aufnehmen: tobias.eibach@uni-ulm.de
oder O27 Zimmer 532.

Webseite: http://www.uni-ulm.de/in/theo/mitarbeiter/eibach/kryptop09.html